UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/549,551	04/14/2000	Takayuki Hasebe	1341.1044/JDH	9207

21171 7590 12/10/2003

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	5

DATE MAILED: 12/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/549,551	HASEBE ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 14 April 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: 'Apparatus to create and verify digital signatures having a secure time element and an identifier of the apparatus'.

Claim Objections

2. Claim 6 is objected to because of the following informalities: the sentence defining the claim is not grammatical. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The invention disclosed in the dependent claim 6 defines a signature creating unit which creates a digital signature only when the confirming unit confirms that the clock works normally (see claim 5), and also, the signature creating unit creates a digital signature using connected information which does not include the time information and a key other than the key used only for creating the signature when the confirming unit confirms that the clock does not work normally (see claim 6). The

later feature of the invention does not comply with the former feature. For the purpose of this action, the examiner will interpret the signature creating unit as outlined in claim 6 as having the later feature.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford U.S. Patent No. 5,189,700 (hereinafter Blandford) in view of Hartman, Jr. U.S. Patent No. 5,444,780 (hereinafter Hartman). As per claim 1, Blandford discloses a signature creating apparatus which creates a digital signature (see Blandford, col. 7, lines 17-22), the signature creating apparatus comprising:

a. a clock (see Blandford, Figure 1, Reference No. 13);

b. a connection unit which connects the time information and an apparatus ID for specifying the creating apparatus to a plain-text and creates a connection data (see Blandford, Figure 1, Reference Nos. 9, 12, 13, 14 and related text; col. 2, line 58-col. 3, line 6); and

c. a signature creating unit which creates the digital signature using the connection data created by the connecting unit and a key used only for creating a signature (see Blandford, Figure 1, Reference Nos. 8, 9, 10, 11 and related text).

Blandford does disclose that the clock is to be non-resettable without execution of a carefully prescribed procedure, but does not elaborate further on the resetting steps (see Blandford, col. 3, lines 24-28). Hartman teaches a timekeeping authority system wherein a trusted time authority initializes the timekeeping facilities of its clients (see Hartman, col. 2, line 65-col. 4, line 10, especially col. 2, line 65-col. 3, line 17). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the time information to only be set by a time authentication authority. Motivation for such an implementation would ensure that only a trusted party makes changes or updates to the clock used in the signature creation steps. The aforementioned covers claim 1.

2. As per claim 10, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises a setting unit which sets the time information according to a time setting request, the setting unit being installed in the time authentication authority (see Hartman, Figure 2, Reference No. 224 and related text; col. 3, line 46-col. 4, line 10; col. 4, line 64-col. 5, line 36).

3. As per claim 11, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises a correcting unit which corrects the clock automatically, the correcting unit being installed in the time authentication authority (see Figure 2, Reference No. 224 and related text; col. 3, lines 4-9 and 34-62).

4. Claims 2, 3, 5, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman as applied to claim 1 above, and further in view of Fisher U.S. Patent No. 5,422,953 (hereinafter Fisher). As per claim 2, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of connecting personal identification information for identifying a person who has created the digital signature to the plaintext. Fisher discloses a personal time notary device wherein a user's identification is appended to the signed message (see Fisher, Figure 3, Reference No. 62 and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to append a personal identification value of the individual who created the digital signature to the plaintext in addition to the time information and apparatus ID. Motivation for such an implementation would enable an auditor to trace the origin of the digital signature back to the individual who created it. Hence, this feature further enhances the credibility of the digital signature creating apparatus.

5. As per claim 3, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises:

a. a storage unit which stores the personal identification information (see Fisher, col. 2, lines 32-37; col. 8, lines 3-33; Figure 1);

b. a judging unit which judges as to whether or not a person who updates stored contents of the storage unit is a person who has proper right; and

c. an updating unit which updates the stored contents of the storage unit only when the judging unit has judged that the person who updates is the person who has proper right (see Blandford, col. 6, lines 41-53).

6. As per claim 5, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of the apparatus creating a digital signature only when the confirming unit confirms that the clock works normally. Fischer discloses a personal date/time notary device wherein the device comprises a confirming unit that confirms a working state of the clock and creates a digital signature only when the confirming unit confirms that the clock works normally (see Fischer, col. 4, lines 42-63, especially lines 46-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Fischer to the apparatus of Blandford. Motivation for such an implementation would enable the invention to prevent the creation of faulty digital signatures based on an invalid timestamp.

7. As per claim 8, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). In addition, the confirming unit confirms the working state of the clock based on a result of comparing a time-counted result of the clock before certain time and a time-counted result at current time (see Fischer, col. 4, line 64-col. 5, line 29).

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman as applied to claim 1, and further in view of Ugon U.S. Patent No. 4,295,041 (hereinafter Ugon). As per claim 4, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Blandford does not stipulate where the apparatus ID is stored; however, the only possible storage locations are either the RAM or the PROM (see Blandford, Figure 1, Reference Nos. 10 and 12). It is well known in the art for sensitive information to be stored in a read only memory to prevent unscrupulous users from modifying the sensitive information. For example, Ugon discloses an apparatus wherein the sensitive information is stored in the PROM (see Ugon, Figure 1, Reference No. 2 and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made for the apparatus ID to be stored in the unrewritable storage unit. Motivation for such an implementation would ensure that the ID is not tampered with after it is initially stored.

9. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer as applied to claim 5, and further in view of Böll U.S. Patent No. 4,230,958 (hereinafter Boll). As per claim 7, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of confirming the working state of the clock based on a result of comparing a driving voltage of the clock with a threshold. However, in the analogous art of semiconductor detector circuits, Boll teaches an invention wherein the working property of a clock is determined by comparing the voltage of the clock with a threshold value (see Boll, Abstract; col. 1, lines 23-44). It would be obvious to one of ordinary skill in the art at the time the invention was made to confirm the working state of the clock based on a result of comparing a driving voltage of the clock with a threshold. Motivation for such an implementation would enable the invention to determine clock operation based on a sample measurement of the clock's driving voltage. This clock confirmation is distinct from other clock confirmation steps in that it checks if the clock is properly furnishing expected periodic pulses (see Boll, col. 1, lines 35-40).

10. Claims 13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman as applied to claim 1, and further in view of Oishi U.S. Patent No. 6,298,153 (hereinafter Oishi) and EAS "The Arithmetic and Logic Unit (ALU)" (hereinafter EAS). As per claim 15, Blandford covers a signature apparatus as outlined above in the claim 3 rejection under 35 U.S.C. 103(a). Blandford is silent on

the matter of a validation method being incorporated in the digital signature apparatus. However, the implementation of a signature validation method that corresponds to a signature creation method is well implemented in the art. As an example, Oishi discloses a digital signature method that generates a digital signature and also comprises a signature verification unit that verifies interpolation using the digital signature, the plaintext and a key (see Oishi, Figure 2, Reference No. 30; col. 11, line 58-col. 12, line 2; col. 12, lines 41-42). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement a signature verification unit in the digital signature apparatus wherein the verification unit verifies interpolation using the digital signature, the plaintext, and a key. Motivation for such an implementation would enable the creator of the signature to verify a signature it has created. Further, Oishi does not specify a function selecting switch which controls the operation of the signature verification and creation modes of the apparatus. However, the implementation of a switch to specify an active operating mode is a conventional feature of any mechanized apparatus having a plurality of modes. For example, in the analogous art of computer logic design, EAS teaches a mode select enabler to make active an operating mode in an ALU having a plurality of modes (see EAS, 2nd and 3rd Figures and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention disclosed by Blandford to implement a function selecting switch which controls the operation of the signature verification and creating modes of the apparatus. Motivation for such an implementation would enable the apparatus to provide both creation and verification services in one machine, thereby

sharing resources among the plurality of services. Furthermore, information required by the validation routine can be stored locally by the creation routine. Finally, the invention disclosed by Oishi discloses a receiving unit that receives the plaintext to which the digital signature is connected (see Oishi, Figure 2). The aforementioned covers claim 15.

11. As per claim 13, it is an apparatus claim corresponding to claim 15 and it does not teach or define above the information claimed in claim 15. Therefore, claim 13 is rejected under Blandford in view of Hartman, Oishi, and EAS for the same reasons set forth in the rejection of claim 15.

12. Claims 12, 14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman, Oishi, and EAS as applied to claim 15, and further in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 16, Blandford covers a signature apparatus as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the switching unit switches a function as a lower apparatus and a function as an upper apparatus; and a key generating unit that generates a key used only for verification of the signature based on an apparatus ID for specifying another signature apparatus which is the lower apparatus and where the signature creating function is made effective when the key generating unit is switched so as to function as the upper apparatus by the switching unit and the signature verification function is made effective by the function selecting unit (see Oishi,

Figure 2 and related text as modified by EAS, 2nd and 3rd Figures and related text). The apparatus disclosed by Blandford implements a public key methodology and not a common key method as specified in the applicant's claim (see Blandford, col. 6, lines 4-7). However, common key methods to sign and verify messages are well-known methods in the digital signature art. For example, Schneier teaches a method to sign documents using symmetric cryptosystems (see Schneier, pages 35-37, 'Signing Documents with Symmetric Cryptosystems and an Arbitrator'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the keys used in creation and verification of a signature be based on a common key method. Motivation for such an implementation would enable the invention to implement a well tested digital signature methodology that features all of the desirable attributes of a paper signature (see Schneier, page 36, characteristics 1-5). The aforementioned covers claim 16.

13. As per claim 14, Blandford covers a digital signature apparatus as disclosed above in the claims 13 and 16 rejections under 35 U.S.C. 103(a). Blandford is silent on the matter of the key generating unit receiving cryptographic information to generate the key for verification. However, as taught by Schneier in a separate section, keys are typically encrypted when keys are transferred from a KDC to a user to keep the key hidden from others (see Schneier, page 176, 'Transferring Keys', 'Key-Encryption Keys'). This encrypted key method requires cryptographic information to be sent to the receiver, namely the encrypted key, whereby this cryptographic information is used to

generate the key. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the key generating unit to receive cryptographic information to generated the key for verification. Motivation for such an implementation would enable the key generating unit to dynamically generate a key having a value distinct from previously generated keys.

14. As per claim 12, it is an apparatus claim covered by the invention covered in the claim 16 rejection and it does not teach or define above the information defined in the invention as outlined in the claim 16 rejection. Therefore, claim 12 is rejected under Blandford in view of Hartman, Oishi, EAS, and Schneier for the same reasons set forth in the rejection of claim 16.

15. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer as applied to claim 5, and further in view of Schneier and Ardon U.S. Patent No. 5,115,425 (hereinafter Ardon). As per claim 6, Blandford covers a signature apparatus as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of the signature creating unit creating a digital signature using a different means if the clock does not work normally. However, this feature of invoking alternative methods when the primary method will not work is well implemented. For example, in the analogous art of a distributed call switching, Ardon teaches an apparatus that switches from one process mode to another when a system failure disables the proper operation of the former process mode (see Ardon, col. 3,

lines 19-28). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the signature creating unit to create a digital signature using a different means if the clock does not work normally. Motivation for such an implementation would ensure continuous reliable service as taught by Ardon (see Ardon, col. 1, lines 15-23). Further, Blandford is silent on the matter of implementing a digital signature that does not use a time element when the clock is not working properly. However, methods to create signatures without incorporating a time element are well known in the art. As an example, Schneier discloses several general digital signature creation techniques that do not include a time element (see Schneier, pages 34-38, 'Digital Signatures'. It would be obvious to one of ordinary skill in the art at the time the invention was made to create a digital signature without a time element. Motivation for such an implementation would enable the invention to provide continuous service using a simple, well-known technique, albeit a service that is less secure in certain circumstances as taught by Schneier. Finally, Blandford is silent on the matter of an alternative digital signature creation method that includes a key other than the key used only for creating the signature. However, as taught by Schneier in a different section, controlling a key's usage is a desirable feature in a secure system to limit the key's exposure (see Schneier, page 180, 'Controlling Key Usage'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a key other than the key used only for creating the signature in the alternative digital signature creation method. Motivation for such an implementation safeguards the privacy of the keys used for different modes of signature creation.

16. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer as applied to claim 5, and further in view of Whitely U.S. Patent No. 4,254,469 (hereinafter Whitely). As per claim 9, Blandford covers a signature creating apparatus which creates a digital signature as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of a flag to indicate whether or not the clock is functioning properly. However, the incorporation of a flag to indicate whether a failure has or has not occurred in the system is a conventional feature of the art. As an example, in the analogous art of error correction, Whitely discloses an invention that sets a flag to indicate a system failure wherein the flag generates an abort response when the flag is set (see Whitely, col. 5, lines 54-60). It would be obvious to one of ordinary skill in the art the time the invention was made to incorporate the teaching of Whitely into the apparatus of Blandford. Motivation for such an implementation would enhance the problem-resolving feature of the invention by providing a single point in the apparatus that indicates if a digital signature was not created due to a failure of the clock.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Fischer U.S. Patent No. 5,136,643 discloses a public/key date-time notary facility.

Haber et al. U.S. Patent No. 5,136,646 discloses a digital document time-stamping with certificate.

Shin et al. U.S. Patent No. 6,072,874 discloses a signing method and apparatus.

Byrd U.S. Patent No. 6,081,899 discloses a time stamping authority hierarchy and associated validating system.

Walker et al. U.S. Patent No. 6,289,453 discloses a method and apparatus for secure measurement certification.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
December 1, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100